I hereby certify that this correspondence is being filed via EFS-Web with the United States Patent and Trademark Office on February 27, 2007.

TOWNSEND and TOWNSEND and CREW LLP

By: /Bonnie Rickles/
Bonnie Rickles

PATENT
Attorney Docket No. 020375-043300US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No. 3753
Justin Monk et al.	Examiner: Thu Thao Havan
Application No.: 10/690,394	Technology Center/Art Unit: 3691
Filed: October 20, 2003	APPELLANTS' BRIEF UNDER 37 CFR §41.37
For: SYSTEMS AND METHODS FOR FRAUD MANAGEMENT IN RELATION TO STORED VALUE CARDS	

Mail Stop Appeal Brief
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Further to the Notice of Appeal mailed on November 20, 2006 for the above-referenced application, Appellants submit this Brief on Appeal.

1. REAL PARTY IN INTEREST

First Data Corporation is the real party in interest as the assignee of the above-identified application.

2. RELATED APPEALS AND INTERFERENCES

No other appeals or interferences are known that will directly affect, are directly affected by, or have a bearing on the Board decision in this appeal.

3. STATUS OF CLAIMS

Claims 1, 2, 4-6 and 8-21 are currently pending in the application. All of these claims stand rejected pursuant to the Office Action mailed June 19, 2006 and have been at least twice rejected.

The rejection of each of Claims 1, 2, 4-6 and 8-21 are believed to be improper and is the subject of this appeal.

4. STATUS OF AMENDMENTS

No claim amendments have been filed subsequent to the mailing of the Office Action of June 19, 2006. A Response to this Office Action, which did not include a claim amendment, was mailed August 21, 2006. The Response prompted a Advisory Action mailed October 5, 2006, in which the claim rejections from the June 19th Office Action were maintained.

5. SUMMARY OF CLAIMED SUBJECT MATTER

Embodiments of the invention relate to fraud management systems and methods to prevent the laundering of stolen funds into stored value products like gift cards (Application p. 1, ll. 12-16). Thieves who traffic in stolen credit card accounts and bank accounts have long understood that they quickly have to convert the funds in these accounts into more anonymous forms of currency such as cash, gold, jewelry, *etc.* More recently, they have exploited the relative anonymity of stored value products, which may be purchased in merchant stores and over the Internet without having to provide a name, address, telephone number, or other type of personal identification. Thus, conversion of stolen funds into stored value products is becoming an increasing problem for consumers, merchants and law enforcement.

Thieves also like stored value products because they can purchase them in a way that circumvents conventional methods of fraud detection based on a payment account's "transaction velocity." A transaction velocity may be determined from the number of transactions being conducted with the account over a predefined period, the amount transacted over the period, *etc.* (Application p. 10, ll. 13-28). Accounts that have a suspiciously high

transaction velocity may be flagged as potentially being involved in fraudulent transactions (Application p. 10, l. 29 to p. 11, l. 4). To avoid raising suspicion, the thieves spread out their fraudulent transactions among several stored value products issued by different issuers. Because the issuers have little information about who is using the card, and do not communicate with each other, the transaction velocity for each stored value card appears normal.

Embodiments of the invention address this security weakness in transaction velocity measurements with systems that have analysis engines that can determine a transaction velocity from transactions made with different stored value products from different issuers (Application p. 2, ll. 2-10). This requirement is fundamental to addressing a security weakness in transaction velocity measurements when fraudulent transactions are spread out over multiple stored value products from multiple issuers. Embodiments of the invention include systems and methods for calculating a transaction velocity from transactions using stored value products from different issuers to close this security loophole (Application p. 3, ll. 11-12).

Independent Claim 1

Independent Claim 1 recites an account acquisition fraud management system that includes a second analysis engine that is "operable to recognize a common load source account to associate the transactions and determine a transaction velocity from the first and second transaction information" (Application p. 10, ll. 18-24). The first transaction information is "about a first transaction with the first stored value product" and the second transaction information is "about a second transaction with the second stored value product," where the second stored value product is "from a different issuer than an issuer of the first stored value product" (Application p. 2, ll. 2-10). Thus, Claim 1 addresses the security weakness described above by determining a transaction velocity from transactions on different stored value products from different issuers.

The system in Claim 1 also includes a cross monitor that is operable to accept the first transaction information from a first analysis engine about the first transaction with the first stored value product, and the second transaction information from the second analysis engine about a second transaction with the second stored value product issued by a different issuer than the first

stored value product (Application, p. 7. ll. 17-24). The cross monitor provides the first transaction information to the second analysis engine, which determines a transaction velocity from both the first and second transaction information after recognizing that there is a common load source account to associate the transactions (Application p. 10, ll. 15-24). If the second analysis engine finds that the transaction velocity exceeds a velocity threshold, it can stall the second transaction (Application p. 11, ll. 15-17). An overview of an embodiment of the system is shown in Fig. 1.

Independent Claim 6

Independent Claim 6 describes a method for detecting fraud in relation to stored value products, where the method includes the steps of receiving a first suspicious activity indication from a first issuer analysis engine that is operable to monitor the activities of a first plurality of stored value products, and receiving a second suspicious activity indication from a second issuer analysis engine that is operable to monitor the activities of a second plurality of stored value products (Application p.2, l. 30 to p. 3, l. 7). The first and second plurality of stored value products are associated with different issuers (Application p. 2, l. 31 to p. 3, l. 2), and the method addresses the security weakness described above by calculating a transaction velocity for a current transaction based the transaction and the suspicious activity indications from the different first and second issuers (Application p. 3, ll. 5-12). Thus, Claim 6 also address the security weakness in determining a transaction velocity by using information associated with at least two different stored value product issuers to calculate the transaction velocity.

The method in Claim 6 also includes the step of associating the first suspicious activity indication and the second suspicious activity indication in a global negative file based on a common load source account used load value on the plurality of the first and the second stored value products (Application p. 3, ll. 2-12). When an activity request that includes transaction information about a current transaction is received from the first issuer analysis engine, the global negative file is accessed to identify the common load source account based at least in part on the transaction information (Application p. 3, ll. 5-11). The method further includes associating the transaction with the first and second suspicious activity indications and

calculating the transaction velocity based on the suspicious activity indications as well as the transaction (Application p. 3, ll. 8-12). Using the calculated transaction velocity, the method calls for providing a response indicating whether the current transaction exceeds a velocity threshold (Application p. 10, l. 29 to p. 11, l. 4). An overview of an embodiment of the method is shown generally in Figs. 2A-B.

Independent Claim 16

Claim 16 describes a system for suppressing fraudulent activity in relation to account acquisition (Application p. 1, l. 29 to p. 2, l. 1). The system addresses the security weakness in determining a transaction velocity by having a cross monitor that is operable to associate information from different monitors associated with different issuers with a transaction, and using this information to determine a transaction velocity for the transaction (Application p. 2, ll. 1-14). Thus, information from different issuers is combined to determine a transaction velocity, thwarting attempts to reduce a calculated transaction velocity by spreading around transactions on stored value products associated with different issuers.

The system of Claim 16 also includes first load and enrollment monitors associated with the first issuer and second load and enrollment monitors associated with the second issuer (Application p. 3, ll. 13-24). The cross monitor uses common load source account information to associate information from the first load or enrollment monitor and the second load or enrollment monitor with the transaction, and then use this information to determine the transaction velocity for the transaction (Application p. 3, ll. 17-24). The cross monitor is also operable to communicate the determined transaction velocity to both the first and second issuers (Application p. 3. ll. 19-21).

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether Claims 1, 2, 4-6 and 8-21 are unpatentable under 35 U.S.C. § 102(e) over U.S. Patent No. 6,714,918 ("Hillmer"). Pages 2 through 6 of the Office Action mailed December 28, 2005, and pages 2 and 3 of the Office Action mailed June 19, 2006 describe the Examiner's position on this issue.

7. ARGUMENT

For a claim rejection to be maintained under 35 U.S.C. § 102(e), the Examiner must find that each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. MPEP § 2131. In the present rejection, the Examiner cites Hillmer as teaching every element of Claims 1, 2, 4-6 and 8-21. In the case of Claim 1, this means that Hillmer has to expressly or inherently describe an analysis engine that is operable to determine a transaction velocity from transactions made on different stored value products from different issuers.

Hillmer did describe calculating a transaction velocity to perform a velocity check against a customer (*see* col. 9, lns. 21-32). However, Hillmer used a conventional method to calculate the transaction velocity that did not include transactions from two or more stored value products from different issuers. The reference calculated a "count velocity" based on the frequency of use of a particular payment instrument (*e.g.*, a credit card number) over a specified period of time, and a "amount velocity" based on frequency of transactions of a particular value (Hillmer col. 9, ll. 21-31). If the calculated transaction velocities exceeded a threshold value then points would be added to a "fraud multiplier" that is used to determine if a transaction may be fraudulent (Hillmer col. 10, ll. 49-53).

There was no description in Hillmer of calculating a transaction velocity by aggregating the number or amounts of transactions made with different payment instruments (*e.g.* stored value cards) issued by different issuers. Instead, Hillmer's transaction velocity calculations relied on aggregating transactions based on "customer 102 identities, credit card account numbers, checking account numbers and addresses, cardholder, ship-to or otherwise (e.g., the frequency of address changes)" (Hillmer col. 9, ll. 32-35). These identifiers would not aggregate the transactions of the thief who spreads out transactions among several anonymous stored value accounts. Each stored value product has a different account number, and information about the product user is generally not provided. There is nothing in the description of transaction velocity calculation in Hillmer that indicates stored value products from different

issuers are aggregated in the calculation, allowing a thief to keep the calculated transaction velocities for each stored value product low enough to avoid fraud detection.

In the Advisory Action mailed October 5, 2006, the Examiner counters this deficiency in Hillmer by noting a passage in the reference (col. 3, lns. 28-35) that states multiple vendors can pool information resources to enhance the detection of fraud:

> Alternatively, most of the fraud detection processing is offloaded to a consumer information provider. Where the consumer information provider is an entity external to the vendor, costs, maintenance, storage and processing considerations are alleviated for the vendor. In addition, centralization of the fraud detection process allows multiple vendors to pool information resources thereby enhancing the detection of fraud.

The Examiner is apparently trying to argue that the description of a conventional transaction velocity calculation, which does not include transactions on stored value products from different issuers, combined with a suggestion that the pooling of information resources by multiple vendors enhances the detection of fraud, is a complete description of an analysis engine that is operable to determine a transaction velocity from transactions made on different stored value products from different issuers. The Appellants disagree that these descriptions in Hillmer either expressly or inherently described a system or method of determining a transaction velocity from transactions made on different stored value products from different issuers.

First, the combination of these passages cannot constitute an express description in Hillmer of a system or method of determining a transaction velocity from transactions made on different stored value products from different issuers. Nowhere in Hillmer was the determination of a transaction velocity explicitly described in this way. Second, for this element to be inherently described by the combination of passages, they must make clear that the missing descriptive matter is necessarily present in Hillmer. See MPEP § 2112, Part IV. However, a suggestion that the pooling of information resources by multiple vendors enhances the detection of fraud is far from specific enough to inherently describe the determination of a transaction velocity from transactions made on different stored value products from different issuers. Hillmer described several factors in addition to transaction velocity that could be used to determine whether a transaction was fraudulent. These included customer information

associated with the transaction, negative credit card or checking account numbers associated with the transaction, negative addresses associated with the transaction, and fraud multiplier points assigned by each vendor, among other factors. *See, e.g.*, Fig 2B in Hillmer and the accompanying description in the Specification. The suggestion to pool information resources by multiple vendors to enhance fraud detection could be applied to any of these factors, and there was no more specific suggestion to pool the information resources when calculating transaction velocity. Even if the combination of passages were to suggest the possibility of determining a transaction velocity this way, that would not be sufficient to establish the inherency of that result or characteristic. See MPEP § 2112, Part IV ("The fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic.")

Thus, Hillmer did not expressly or inherently describe a system or method of determining a transaction velocity from transactions made on different stored value products from different issuers. For at least this reason, Claim 1, and Claims 2, 4 and 5, which depend of Claim 1, are allowable over the reference.

For a similar reason, the rejection of Claims 6 and 16 under 35 U.S.C. § 102(e) over Hillmer should be withdrawn. Claim 6 describes a method for detecting fraud in relation to stored value products, where the method includes the steps of receiving a first suspicious activity indication from a first issuer analysis engine that is operable to monitor the activities of a first plurality of stored value products, and receiving a second suspicious activity indication from a second issuer analysis engine that is operable to monitor the activities of a second plurality of stored value products. The first and second plurality of stored value products are associated with different issuers, and the method addresses the security weakness described above by calculating a transaction velocity for a current transaction based the transaction and the suspicious activity indications from the different first and second issuers. Claim 16 describes a system for suppressing fraudulent activity in relation to account acquisition. The system addresses the security weakness in determining a transaction velocity by having a cross monitor that is

operable to associate information from different monitors associated with different issuers with a transaction, and using this information to determine a transaction velocity for the transaction.

In both Claims 6 and 16, a transaction velocity is determined from activity associated with different stored value products from different issuers. As noted above, Hillmer neither expressly nor inherently described this element of Claims 6 and 16, making these claims allowable over the reference. For at least the same reason, Claims 8-15, and 17-21, which depend from Claims 6 and 16, respectively, are also allowable over Hillmer.

8. CONCLUSION

Appellant believes that the above discussion is fully responsive to all grounds of rejection set forth in the application. For the reasons set forth above, it is respectfully submitted that the rejection should be reversed. The fees for filing this Brief are enclosed herewith, and no other fees are believed due. Should the Office determine otherwise, however, it is authorized to deduct any requisite fees from Deposit Account 20-1430 that may be due in association with the filing of this appeal and Brief.

Respectfully submitted,

/Eugene J. Bernard/
Eugene J. Bernard
Reg. No. 42,320

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 650-326-2422
60979713 v1

9. CLAIMS APPENDIX

1. (Previously presented) An account acquisition fraud management system, the account acquisition fraud management system comprising:

a first analysis engine, wherein the first analysis engine is associated with a first stored value product;

a second analysis engine, wherein the second analysis engine is associated with a second stored value product from a different issuer than an issuer of the first stored value product; and

a cross monitor, wherein the cross monitor is operable to accept a first transaction information from the first analysis engine about a first transaction with the first stored value product and a second transaction information from the second analysis engine about a second transaction with the second stored value product, wherein the first transaction information is provided from the cross monitor to the second analysis engine; and

wherein the second analysis engine is operable to recognize a common load source account to associate the transactions and determine a transaction velocity from the first and second transaction information, and stalling the second transaction when the transaction velocity exceeds a velocity threshold.

2. (Original) The system of claim 1, wherein the system further comprises:

a computer readable medium accessible to the cross monitor, wherein the computer readable medium includes the first transaction information and the second transaction information.

3. (Cancelled)

4. (Original) The system of claim 1, wherein the first transaction information and the second transaction information are selected from a group consisting of:

a physical address;

a telephone number;

a virtual address; and

a load source.

5. (Original) The system of claim 1, wherein the cross monitor is further operable to maintain the first transaction information is a queue associated with an issuer of the second stored value card product.

6. (Previously presented) A method for detecting fraud in relation to stored value products, the method comprising:

receiving a first suspicious activity indication from a first issuer analysis engine, wherein the first issuer analysis engine is operable to monitor activities occurring in relation to a first plurality of stored value products associated with the first issuer;

receiving a second suspicious activity indication from a second issuer analysis engine, wherein the second issuer analysis engine is operable to monitor activities occurring in relation to a second plurality of stored value products associated with a second issuer different from the first issuer;

associating the first suspicious activity indication and the second suspicious activity indication in a global negative file based on a common load source account used load value on the plurality of the first and the second stored value products;

receiving an activity request from the first issuer analysis engine, wherein the request includes a transaction information about a current transaction with one of the first plurality of stored value products associated with the first issuer;

based at least in part on the transaction information, accessing the global negative file, wherein the transaction information includes the identity of the common load source account;

associating the current transaction with the first suspicious activity indication and the second suspicious activity indication and calculating a transaction velocity based on the transaction information, and the first and second suspicious activity indications in the global negative file; and

providing a response, wherein the response indicates whether the current transaction exceeds a velocity threshold.

7. (Cancelled).

8. (Original) The method of claim 7, wherein the transaction information is selected from a group consisting of:

a physical address;

a telephone number;

a virtual address; and

a load source.

9. (Original) The method of claim 6, wherein the transaction information is a physical address.

10. (Original) The method of claim 6, wherein the transaction information is a telephone number.

11. (Original) The method of claim 6, wherein the transaction information is a virtual address.

12. (Original) The method of claim 6, wherein the response is maintained in a queue associated with the first issuer.

13. (Original) The method of claim 12, wherein the response includes at least two of the following:

a date of the suspicious behavior;

a funding account number;

a denial reason;

a review status; and

a reviewer note.

14. (Original) The method of claim 12, wherein the response includes an indication of related accounts.

15. (Previously presented) The method of claim 6, wherein the response is a first response associated with a first account, wherein the global negative file includes information about a second account having one or more items of the transaction information in common with the first account, and wherein the method further comprises:

identifying the second account using the transaction information, and providing a second response to the second issuer associated with the second account.

16. (Previously presented) A system for suppressing fraudulent activity in relation to account acquisition, the system comprising:

a first load monitor associated with a first issuer;

a second load monitor associated with a second issuer;

a first enrollment monitor associated with the first issuer;

a second enrollment monitor associated with the second issuer; and

a cross monitor, wherein the cross monitor is operable to associate information from the first load monitor or first enrollment monitor, and the second load monitor or second enrollment monitor with a transaction using a first stored value product using common load source account information, and wherein the cross monitor is operable to determine a transaction velocity for the transaction using the information, and communicate the transaction velocity to both the first issuer and the second issuer.

17. (Original) The system of claim 16, wherein a request to load value on a stored value product associated with the first issuer is processed at least in part by the first load monitor.

18. (Original) The system of claim 17, wherein the first load monitor is operable to apply a velocity check on a load request.

19. (Previously presented) The system of claim 16, wherein the first load monitor is further operable to compare the transaction velocity with a predefined velocity limit.

20. (Original) The system of claim 19, wherein the first load monitor is operable to provide a detected suspicious activity to the cross monitor.

21. (Previously presented) The system of claim 20, wherein the detected suspicious activity is that the transaction velocity has exceeded the predefined velocity limit.

10. EVIDENCE APPENDIX

None

11. RELATED PROCEEDINGS APPENDIX

None